DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD, SUITE 2533
FT. BELVOIR, VIRGINIA 22060-622 1

OCT 7 1998

IN REPLY REFER TO CII

MEMORANDUM FOR CA DAPSC DCMC DLSC FO GC

SUBJECT: Information Vulnerability and the World Wide Web

On 24 September 1998, the Deputy Secretary of Defense issued a memorandum on information vulnerability and the World Wide Web. The memo identifies the types of information which must be removed from publicly accessible web sites to minimize the risk of information being aggregated for possible use by our adversaries to threaten DoD systems and personnel.

Consistent with the Deputy Secretary Defense guidance, each organization should initiate a thorough review of any publicly accessible web site (e.g., not password protected or domain restricted) within your area of functional responsibility and ensure that the following types of information are removed immediately:

- Plans or lessons learned which would reveal sensitive military operations, exercises, or vulnerabilities.

- Reference to any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

- All personal information in the following categories about U.S. citizens, DoD employees and military personnel: (1) Social Security Account Numbers; (2) dates of birth; (3) home addresses; and (4) telephone numbers other than numbers of duty offices which are appropriately made available to the general public. In addition, remove names, locations, and any other identifying information about family members of DoD employees and military personnel.

Additionally, organizations should ensure steps are taken to review all acquisition information, in the broadest sense, that is made available via on-line public sources for compliance with above. Acquisition information includes, but is not limited to, Commerce Business Daily synopses, requests for proposals, and material on business opportunity, program management, and Integrated Product Team homepages. Program management status information should be screened to ensure that it does not reveal potential program vulnerabilities (e.g., cost, schedule, or technical issues that may inhibit achievement of program objectives, including initial operational capability .)

OCT 7 1998

To comply with the Deputy Secretary of Defense memo, each organization should submit a verification report acknowledging completion of the above actions. Verification reports should include: Organization name, web site(s) reviewed, name and phone number of person certifying verification, date verification completed. Your verification report must identify waivers granted, information waived, and recommendations for addressing technical data issues, if applicable. The Deputy Secretary of Defense guidance provides that a waiver may be granted, on a non-delegable basis, for information to remain on publicly accessible sites if deemed essential to mission accomplishment.

Organizations should also evaluate the sensitivity of technological data included on web sites to assess the extent that such information, when compiled with other unclassified information, reveals an additional association or relationship that meets the standards for classification under Section 1.8(e) E.O. 12958. Please include recommendations for addressing this issue in your verification report.

As a remedial action, organizations should provide a list of all web sites that will be reviewed and the webmaster/point of contact for the site no later than 16 October 98. After which a weekly progress report of web sites reviewed should be provided. The progress report should include the web site name and status (completed/pending review).

Please provide your final verification report (format attached) to Lt Col Bryant, CII, 767-3135 no later than 2 November 1998.

CARLA A. VON BERNEWITZ
Chief Information Officer

Attachments

VERIFICATION REPORT

ORGANIZATION:

FIELD ACTIVITY	WEB SITE(S) (Ex: www.supply.dla.mil/services.htm)	TECHNOLOGY SENSITIVE (Note 1)	WAIVER (Note 2)	DATE COMPLETED	CERTIFIED BY (DAA or Delegated Representative)

TECHNOLOGICAL DATA SENSITIVITY

NOTE 1: If "yes (Y)", assess the extent that such information, when compiled with other unclassified information, reveals additional association. or relationships. Include recommendation for addressing this issue.

WAIVERS GRANTED

NOTE 2: If "yes (Y)", identified information waived and recommendations for addressing data issues.